

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-201143

(P2000-201143A)

(43)公開日 平成12年7月18日(2000.7.18)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 B 5 B 0 1 7
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 K 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 C 5 J 1 0 4
			3 3 0 B 5 K 0 3 0
H 0 4 L 12/28		H 0 4 L 11/00	3 1 0 D 5 K 0 3 3

審査請求 有 請求項の数 3 O L (全 5 頁) 最終頁に続く

(21)出願番号 特願平11-692

(22)出願日 平成11年1月5日(1999.1.5)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 青柳 友一

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100108578

弁理士 高橋 昭男 (外3名)

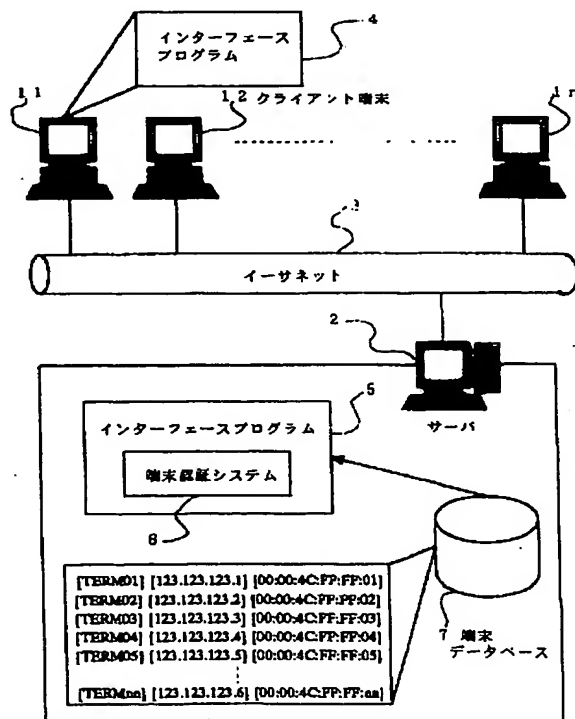
最終頁に続く

(54)【発明の名称】 端末認証装置

(57)【要約】

【課題】 クライアント端末からの不正なアクセスを阻止する機能を、サーバのプログラムのみに持たせればよい端末認証装置を提供する。

【解決手段】 サーバ2とクライアント端末11~1nは、イーサネット(登録商標)3を介して接続されている。サーバ2には、クライアント端末11~1nの端末名、IPアドレスおよびMACアドレスからなるレコードを格納した端末データベース7を備える。また、サーバのインターフェースプログラム5には、クライアント端末11~1nからの呼び出しがあると、その呼び出しプログラムからパラメータとして引き渡されるIPアドレスを基に端末データベース7からMACアドレスを取得し、IPアドレスとMACアドレスの組み合わせが正しいか否かが判定することにより、クライアント端末11~1nの利用権の有無を検査する端末認証システム6を組み込んでいる。



## 【特許請求の範囲】

【請求項1】 SOCKETインターフェースを使用したシステムにおける端末認証装置において、クライアント端末からの呼び出しがあると、サーバにおいて、該呼び出しプログラムからパラメータとして引き渡されるIPアドレスを基に前記クライアント端末のMACアドレスを取得し、IPアドレスとMACアドレスの組み合わせが正しいか否かを判定することにより、前記クライアント端末の利用権の有無を検査することを特徴とする端末認証装置。

【請求項2】 サーバと複数のクライアント端末とがイーサネットを介して接続されたシステムにおける端末認証装置において、

前記サーバには、前記クライアント端末の端末名、IPアドレスおよびMACアドレスからなるレコードを格納した端末データベースを備えるとともに、

前記サーバのインターフェースプログラムにのみ、前記クライアント端末からの呼び出しがあると、該呼び出しプログラムからパラメータとして引き渡されるIPアドレスを基に前記端末データベースからMACアドレスを取得し、IPアドレスとMACアドレスの組み合わせが正しいか否かを判定することにより、前記クライアント端末の利用権の有無を検査する端末認証システムを組み込んだことを特徴とする端末認証装置。

【請求項3】 前記端末データベースのレコードに、ユーザIDとパスワードを付加し、前記端末認証システムは、利用者認証をも行うことを特徴とする請求項2記載の端末認証システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、端末認証装置、SOCKETインターフェースを使用したシステムにおいて、接続してきたクライアント端末のIPアドレスとMACアドレスの組み合わせによって、当該端末の正当性（利用権の有無）を検査するシステムに関する。

## 【0002】

【従来の技術】 従来のこの種の技術として、特開平6-334671公報に記載された「ローカルエリアネットワーク監視システム」を挙げることができる。この技術は、衝突検出型搬送波多重アクセス（CSMA/CD）を用いるイーサネット（ethernet）等のローカルエリアネットワークのセグメントに接続された複数の端末の各々には、それぞれ、たとえばIPアドレスおよびMACアドレスおよび端末名などからなる識別情報を付与して記憶しておくとともに、ネットワーク監視装置の記憶手段には、各端末の識別情報を記憶させておく。そして、端末の電源投入時に、当該端末に関する識別情報を含み、ネットワーク環境を立ち上げたことを示すブロードキャスト信号がセグメントに発行され、ネットワーク監視装置は、このブロードキャスト信号を受信すると、ネ

ットワーク監視装置内の記憶手段の識別情報を検索し、照合する。この時、記憶手段内に受信した当該端末の識別情報が存在する場合には、当該端末のセグメントに対するアクセスを黙認し、特に何も行わない。一方、記憶手段内に当該識別情報が存在しないと判明した場合には、制御論理が自動的に当該端末に対して衝突信号を発行し、当該端末によるLANの利用を阻止し、必要に応じて、利用を阻止した端末に関する識別情報を印字出力するなどの操作を行う。

## 【0003】

【発明が解決しようとする課題】 しかしながら、上述した従来技術では、ネットワーク監視装置（サーバ）側のプログラムと、端末（クライアント）側のプログラムの双方で、IPアドレス、MACアドレス、端末名などの端末の識別情報と、この識別情報を送受信するためのインターフェースを備える必要があるという問題点がある。本発明は、この点に鑑みなされたものであり、クライアント端末からの不正なアクセスを阻止する機能をサーバのプログラムにのみ持たせればよい端末認証装置を提供することを目的とする。

## 【0004】

【課題を解決するための手段】 そのために、第1の本発明の端末認証装置は、クライアント端末からの呼び出しがあると、サーバにおいて、該呼び出しプログラムからパラメータとして引き渡されるIPアドレスを基に前記クライアント端末のMACアドレスを取得し、IPアドレスとMACアドレスの組み合わせが正しいか否かを判定することにより、前記クライアント端末の利用権の有無を検査する。また、第2の本発明の端末認証装置は、サーバと複数のクライアント端末とがイーサネットを介して接続されたシステムにおける端末認証装置において、前記サーバには、前記クライアント端末の端末名、IPアドレスおよびMACアドレスからなるレコードを格納した端末データベースを備えるとともに、前記サーバのインターフェースプログラムにのみ、前記クライアント端末からの呼び出しがあると、該呼び出しプログラムからパラメータとして引き渡されるIPアドレスを基に前記端末データベースからMACアドレスを取得し、IPアドレスとMACアドレスの組み合わせが正しいか否かを判定することにより、前記クライアント端末の利用権の有無を検査する端末認証システムを組み込んだことを特徴とする。本発明では、サーバ側に端末認証システムを組み込むことにより、SOCKETインターフェースを使用したシステムで利用権のないクライアント端末が、IPアドレスを不正に変更し、恰も利用権のある端末に見せて不正なアクセスをすることを防止する。これは、システム内で固有のユーザID/パスワードの仕組みを用いて行うことが通例であるが、従来は、クライアント側のプログラムとサーバ側のプログラムとにその機能を持たせなければならなかった。しかし、本発明では、サー

バのプログラムにのみ端末認証システムを持つことで端末認証が可能となる。

#### 【0005】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。図1を参照すると、本発明の一実施例が示されており、クライアントサーバのシステム構成で使用されることが分かる。すなわち、 $n$ 個のクライアント端末11～1 $n$ とサーバ2とがイーサネット3を介して接続されている。各クライアント端末11～1 $n$ 側には、SOCKETインターフェースプログラム4が備えられているのに対して、サーバ側2には、端末認証システム6が組み込まれたSOCKETインターフェースプログラム5が備えられている。したがって、端末認証システム6は、サーバ2上にのみ存在し、サーバ側のSOCKETインターフェースプログラム5に取り込まれ、1機能として動作する。また、サーバ2には、端末データベース7が設けられている。図1の端末データベース7における各レコードは、端末名、IPアドレス、MACアドレスの順番に並べられた項目からなり、各項目は、かっこ（[]）で括られて1レコードを構成する。例えば、端末名=TERM1、IPアドレス=111.222.111.222、MACアドレス=00:00:4C:FF:FF:FF、という端末があった場合、[TERM1][111.222.111.222][00:00:4C:FF:FF:FF]という定義になる。ファイル形式はメンテナンスの容易性、ファイルI/Oの処理速度を考慮し、テキスト形式の順編成ファイルとする。システム運用にあたって、このようなデータが端末データベース7に予め登録されている必要がある。

【0006】次に、図2を参照して本実施例の動作について説明する。図2は、端末認証システム6のフローチャートを示す。まず、ステップA1において、呼び出し元プログラムからパラメータとして引き渡されたIPアドレスを基に、接続相手となるクライアント端末のMACアドレスを取得する。このとき、ARP(Address Resolution Protocol)を使用する。ステップA2において、IPアドレスをキーワードとして、端末データベース7を検索する。端末データベース7に該当するIPアドレスが存在するか、どうか判定し(ステップA3)、存在しなかった場合は呼び出し元プログラムにNGを返却し、プログラムを終了する(A7)。また、ステップA3において、目的のIPアドレスが存在した場合は、IPアドレスとMACアドレスの組み合わせが正しいかどうかを判定し(ステップA4)、判定の結果正当な端末でなかった場合は呼び出し元プログラムにNGを返却し(A7)、プログラムを終了する。一方、正当な端末であった場合は呼び出し元プログラムにOKを返却し(A6)、プログラムを終了する。

【0007】次に、本発明の他の実施例について説明する。図3を参照すると、この実施例では、端末データベース9におけるレコードは、ユーザID、パスワードを組み合わせている点が図1における端末データベース7のレコードと異なる。これにより、端末認証と端末に対する利用者認証を行え、より信頼性の高い不正アクセス防止が可能となる。

【0008】次に、図4を参照して本実施例の動作について説明する。図4は、図3における端末認証システム8のフローチャートを示す。まず、ステップB1において、呼び出し元プログラムからパラメータとして引き渡されたIPアドレスを基に、接続相手となるクライアント端末のMACアドレスを取得する。このとき、ARP(Address Resolution Protocol)を使用する。ステップB2において、IPアドレスをキーワードとして、端末データベース9を検索する。端末データベース9に該当するIPアドレスが存在するか、どうか判定し(ステップB3)、存在しなかった場合は呼び出し元プログラムにNGを返却し、プログラムを終了する(B9)。また、ステップB3において、目的のIPアドレスが存在した場合は、IPアドレスとMACアドレスの組み合わせが正しいかどうかを判定し(ステップB4)、判定の結果正当な端末でなかった場合は呼び出し元プログラムにNGを返却し(B9)、プログラムを終了する。ここまでの処理は、図2における処理と同一である。図2と図4では、共に端末データベース7または9の検索、即ちファイルI/Oは1度しか行われなため、クライアント端末11～1 $n$ に対する利用者認証の機能を付け加えたとしても、処理速度に大きな影響は与えない。そこで、本実施例では、図4のステップB6、B7において、ユーザIDとパスワードの検査を行っているが、これは呼び出し元プログラムからパラメータとして与えられなければならない、そのためにはクライアント側のSOCKETインターフェースプログラム4の修正も必要となる点に注意された。

#### 【0009】

【発明の効果】本システムを導入すれば、ユーザID/パスワードによる利用者認証機能を有しているシステムであれば、より信頼性の高い不正アクセス防止を実現することができるという効果を得ることができる。また、既に運用に入ってしまったSOCKETインターフェースを利用したシステムでこうした機能を有しないシステムであっても、クライアント端末側のプログラムを修正することなく、サーバ側のプログラムを修正するだけで、端末利用権の検査機能を導入することが可能である。

#### 【図面の簡単な説明】

【図1】 本発明の一実施例のブロック図。

【図2】 図1に示した実施例における端末認証システ

ムのフローチャート。

【図3】 本発明の他の実施例のブロック図。

【図4】 図3に示した実施例における端末認証システムのフローチャート。

【符号の説明】

11、1n クライアント端末

2、20 サーバ

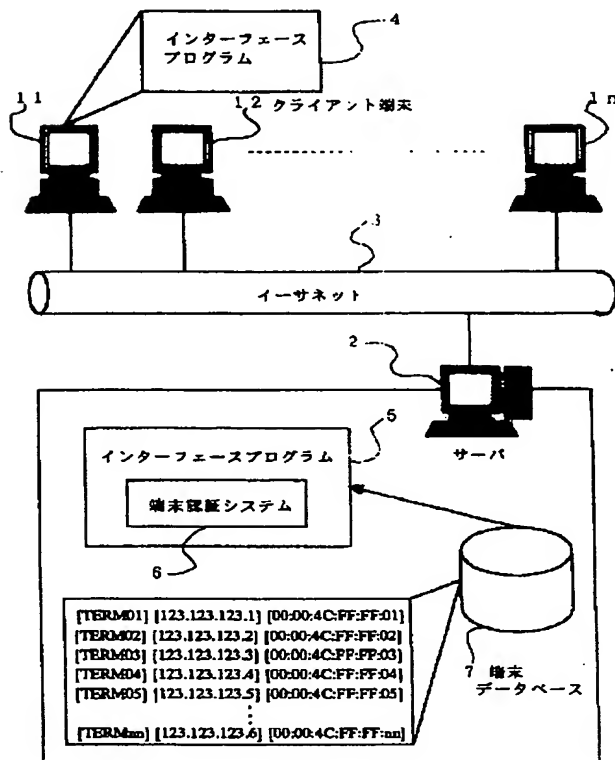
3 イーサネット

4、5 SOCKETインターフェースプログラム

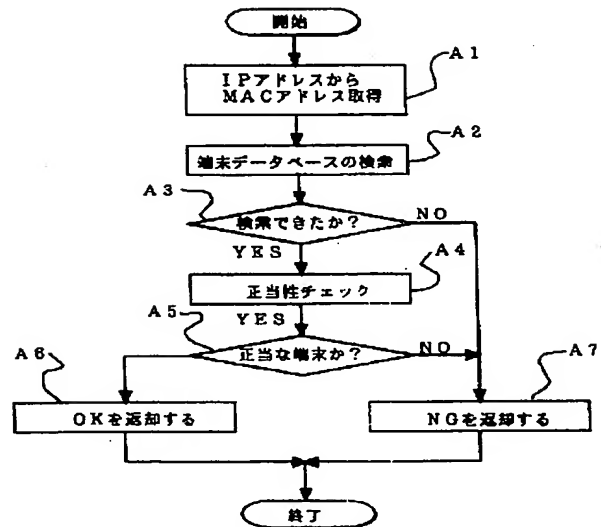
6、8 端末認証システム

7、9 端末データベース

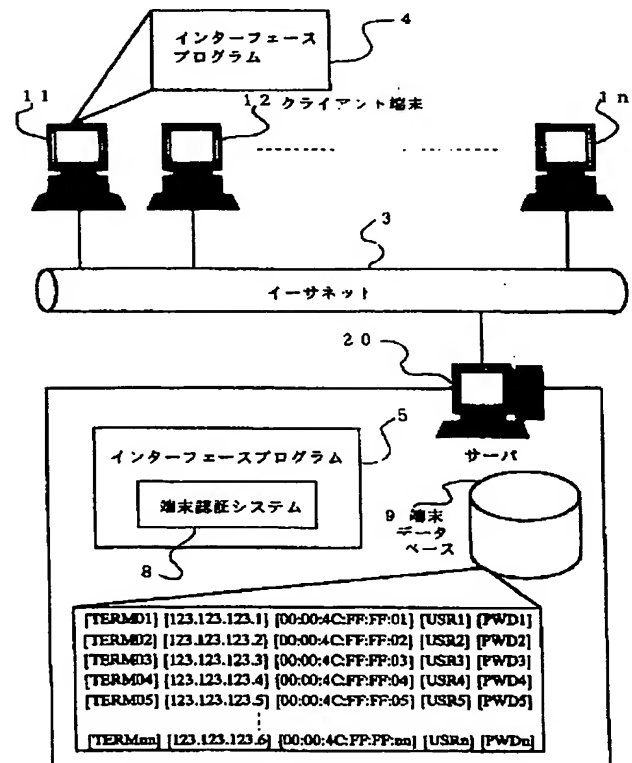
【図1】



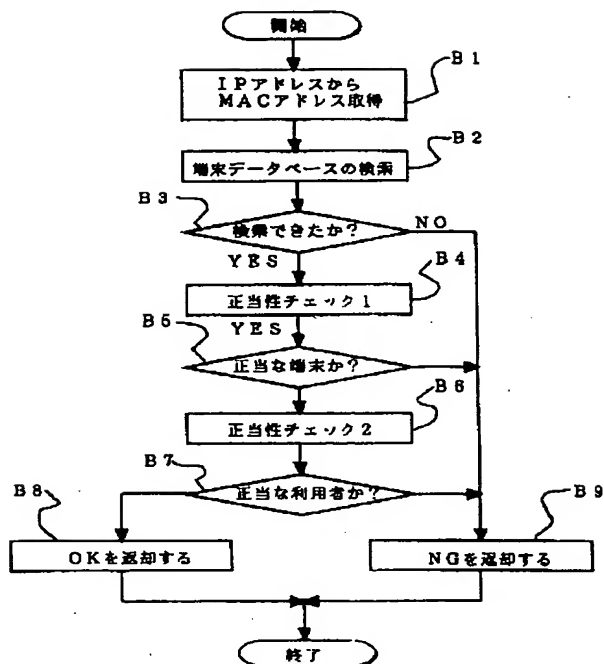
【図2】



【図3】



【図4】



フロントページの続き

(51) Int. Cl. 7

H 0 4 L 12/56

識別記号

F I

H 0 4 L 11/20

テーマコード (参考)

1 0 2 Z

Fターム(参考) 5B017 AA01 BA05 BB02 BB07 CA16  
 5B085 AE04 AE23 BG07  
 5J104 AA07 KA01 KA02 NA00 NA05  
 NA20 PA07  
 5K030 GA15 HC14 HD09 JT02 JT06  
 LB02 LC16 LD19 LD20  
 5K033 AA08 CA08 CB01 DA01 DB20  
 EC01 EC04